

REMARKS/ARGUMENTS

Claims 1-43 are pending. Claims 2, 3, 21, 22, 32 and 33 have been canceled.
Claims 1, 20, 31, and 42 have been amended.

In the Office Action, the Examiner rejected claims 1-43 under 35 USC §103(a) as being unpatentable over Pavlov (4,614,861) in view of Spratte (5,764,766).

I. Claims 1,4-19

Claim 1 is allowable over Pavlov and Spratte, alone or in combination, as those references fail to disclose or suggest all the elements of claim 1. For example, Claim 1 recites:

a digital wallet, secured with a user's access code, for reproducing a confidential datum for said user, said digital wallet comprising:

a computer-implemented input for receiving an input access code; ...

a seed-based data generation module ... configured to generate an output datum ..., and said output datum reproducing said at least a portion of said user's confidential datum if said input access code equals said user's access code; and

wherein for at least one input access code not equaling said user's access code, said output datum has the characteristic appearance of said at least a portion of said confidential datum, but said output datum does not reproduce at least a portion of said user's confidential datum.

In Pavlov, if an incorrect PIN is entered then no further steps are done and no output datum is generated. See column 11 line 62 to column 12 line 11. Thus, Pavlov does not disclose or suggest generating an output datum when the input access code is not equal to the user's access code. Particularly, Pavlov does not disclose an output datum that has the characteristic appearance of the confidential datum, but does not reproduce the user's confidential datum.

Spratte is concerned with combining a salt S (additional text) to a primary secret key K_p , and then hashing the result to create an encryption key K_e in order to create a manageable but secure encryption method. See column 2 line 65 to column 3 line 10. There is

no input access code, and thus no generation of output datum based upon the input access code. Furthermore, Spratte is concerned with creating a one-time encryption key and not reproducing confidential datum. See column 2 lines 53-56. Therefore, in addition to Spratte not disclosing or suggesting generating output datum based on an input access code, Spratte cannot be combined with Pavlov to create a method for reproducing a confidential datum due to Spratte's focus on creating a one-time encryption key.

For at least the reasons stated above, Applicants submit that claim 1 is allowable over the cited references. As claim 1 is allowable, claims 4-19 dependent therefrom are also allowable for at least that reason.

II. Claims 20, 23-30

Claim 20 recites similar features as recited for claim 1, and thus claim 20 should be allowable for at least similar reasons as claim 1. As claim 20 is allowable, claims 23-30 dependent therefrom are also allowable for at least that reason.

III. Claims 31, 34-41

Claim 31 recites similar features as recited for claim 1, and thus claim 31 should be allowable for at least similar reasons as claim 1. As claim 31 is allowable, claims 34-41 dependent therefrom are also allowable for at least that reason.

IV. Claim 42

Claim 42 recites similar features as recited for claim 1, and thus claim 42 should be allowable for at least similar reasons as claim 1.

V. Claim 43

Claim 43 is allowable over Pavlov and Spratte, alone or in combination, as those references fail to disclose or suggest all the elements of claim 43. For example, Claim 43 recites a method comprising "generation-camouflaging at least a portion of said access-controlled datum such as to be reproducible by an authorized user thereof but non-reproducible by an unauthorized user thereof."

"If the user inputs an incorrect PIN, a wrong private key is produced. We refer to private keys protected in this manner as being ""generation camouflaged." See paragraph 13 of the published U.S. patent application no. 2002/0141575.

Appl. No.
Amdt. dated May 4, 2005
Reply to Office Action of February 24, 2005

PATENT

As detailed in the discussion for claim 1, Pavlov does not produce datum if the PIN is incorrect. See column 11 line 62 to column 12 line 11. Thus, Pavlov does not disclose or suggest generation camouflaging.

In Spratte, there is no input access code, and thus no generation of output datum that can depend upon the input access code. Thus, Spratte does not disclose or suggest generation camouflaging.

For at least the reasons stated above, Applicants submit that claim 43 is allowable over the cited references.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 415-576-0200.

Respectfully submitted,
Philip H. Albert
Reg. No. 35,819

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 415-576-0200
Fax: 415-576-0300
Attachments
PHA:sfs
60471627 v1